NCSC-TG-002
VERSION - 1

NATIONAL COMPUTER SECURITY CENTER

TRUSTED PRODUCT EVALUATIONS

A GUIDE FOR VENDORS

22 June 1990

FOREWORD

Trusted Product Evaluations: A Guide for Vendors describes procedures for conducting business with the Information Systems Security Organization within the National Security Agency using the Trusted Product Evaluation Program. The *Vendors' Guide* provides the information needed for the vendor to submit a computer product for information systems security evaluation of its trusted features and assurances and outlines the National Security Agency's responsibilities for timely acknowledgments.

This publication specifically covers the relationship between the National Computer Security Center within the Information Systems Security Organization and the vendors of proposed trusted computer products. It covers the process from the initial contact with the vendor through the completion of the security evaluation and follow-up programs. Although other guidelines will be referenced in this publication, we provide sufficient instructions for any first-time user of the National Computer Security Center's services.

The *Vendors' Guide* is the latest addition to the "Rainbow Series." These publications are the product of the Technical Guideline Program. The National Computer Security Center designed these technical guidelines to provide insight to the *Trusted Computer System Evaluation Criteria* requirements and guidance for meeting each requirement.

The National Computer Security Center has established an aggressive program to study and implement computer security technology. Our goal is to encourage the widespread availability of trusted computer products for use by any organization desiring better protection of their important data. The Trusted Product Evaluation Program focuses on the security features of commercially produced and supported computer systems. We evaluate the protection capabilities against the established criteria presented in the *Department of Defense Trusted Computer System Evaluation Criteria*. This program and an open and cooperative business relationship with the computer and telecommunications industries will result in the fulfillment of our country's information systems security requirements. We resolve to meet the challenge of identifying trusted computer products suitable for use in protecting information.

As the Director, National Computer Security Center, I invite your recommendations for revising this technical guideline. We plan to review this document as the need arises.

PATRICK R. GALLAGHER, JR.

22 June 1990

Director

National Computer Security Center

TABLE OF CONTENTS

1. INTRODUCTION

In January 1981, the Department of Defense assigned the responsibility for computer security to the Director of the National Security Agency (NSA). This action led to the formation of the Computer Security Center. The Computer Security Center's Charter was promulgated in Department of Defense Directive 5215.1 in October 1982. It specifically tasks the Computer Security Center to establish and maintain

> ". . . technical standards and criteria for the security evaluation of trusted computer systems that can be incorporated readily into the Department of Defense component life-cycle management process . . ."

The developmental experiments in the 1970's ranged from attempts to add security front-ends to existing systems, to total design of secure systems and hardware. Early research and development efforts defined a graduated scale of security features and design principles. We incorporated these features and principles in the *Department of Defense Trusted Computer System Evaluation Criteria* (TCSEC).

The National Computer Security Center (NCSC) issued the TCSEC in August 1983. Later, the DoD reissued the TCSEC as a Department of Defense Standard (DOD 5200.28-STD) in December 1985.

The NCSC recognizes the technical challenges involved in providing effective protection within computer operating systems and networks. We rely on an open and cooperative relationship with government, industry representatives, and the academic community to accomplish these important objectives. The government encourages industry to provide the computer security capabilities government needs. The NCSC sponsors critical research and makes the results widely available to encourage their incorporation into trusted computer products and secure applications. We evaluate the security of computer software and hardware products on computer systems produced by industry or the government.

A trusted computer system employs sufficient hardware and software integrity measures to allow it to process simultaneously a range of sensitive information. Information could be unclassified (FOUO, proprietary) or classified (e.g., CONFIDENTIAL through TOP SECRET) for a diverse set of users without violating

access privileges. We base levels of trust on the ability of the computer system to enforce access privileges of authorized users and to protect system files.

The NCSC evaluates the security features and assurances of trusted products against established technical standards and criteria. We also maintain the Evaluated Products List published quarterly as part of the *Information Systems Security Products and Services Catalogue*. The Evaluated Products List is a compilation of all computer products that have undergone formal security evaluations, and it shows the relative security merit of each computer product. To evaluate computer systems, we use the TCSEC as our standard. This provides a metric for distinguishing a range of features and assurances for security controls built into automatic data processing system products. The TCSEC establishes specific requirements that a computer system must meet in order to achieve a specific level of trustworthiness. The TCSEC hierarchically arranges the levels of trust into four major divisions of protection, each with certain security-relevant characteristics. These divisions are subsequently subdivided further into more precise levels of trust.

In recognition of the complex and technical nature of the issues addressed by the TCSEC, the NCSC has established a Technical Guidelines Program. This program augments information provided in the TCSEC by publishing additional guidance on issues and features addressed therein. This set of documents is referred to as the "Rainbow Series."

2. TRUSTED PRODUCT EVALUATION PROGRAM

This section of the *Vendors' Guide* provides the computer product vendor with an overview of the NCSC's Trusted Product Evaluation Program. Our program benefits from the partnership with the vendor. During the five phases of this process, each of us share in the responsibility to a greater or lesser degree to affect the product evaluation. The National Security Agency (NSA) assumes major responsibility during the proposal review, whereas the vendor must accept the lead role during the Vendor Assistance Phase. If each of us provides dedicated resources, together we can develop evaluated trusted products for the U.S. Government and the non-government user community.

SHARED RESPONSIBILITY

"PARTNERSHIP WITH THE VENDOR"

The graph on the following page illustrates the process of a trusted product evaluation for a system or network. This process breaks down into the following phases:

A. The **Proposal Review Phase** is the decision-making process to initiate the program. This phase includes the initial contact between the vendor and Information Systems Security Organization (ISSO) within the National Security Agency (NSA). The signing of a legal agreement culminates this action and launches the product evaluation into the next phase.

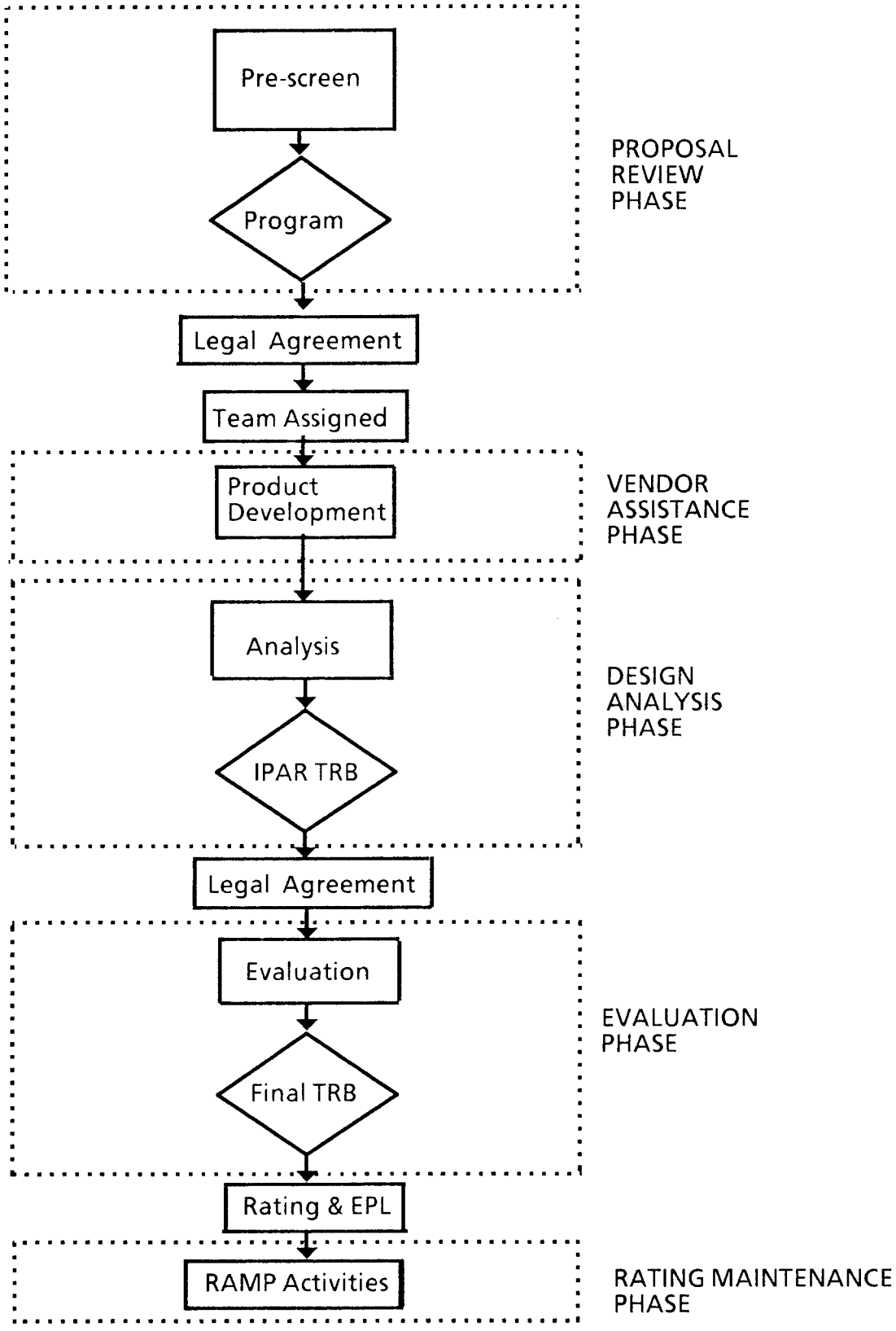
B. The **Vendor Assistance Phase** provides the vendor the opportunity to obtain assistance from the NCSC during the development of a system or network product.

C. The **Design Analysis Phase** allows the NCSC to analyze intensely the product and software design. Another legal agreement is signed before initiation of the next phase.

D. The **Evaluation Phase** consists of the actual security evaluation of the vendor's computer system. Successful completion of this process allows us to place the vendor's computer product on the Evaluated Products List.

E. The **Rating Maintenance Phase** provides a mechanism to ensure the validity of a previous rating for successive versions of an evaluated computer system product.

TRUSTED PRODUCT EVALUATION PROGRAM

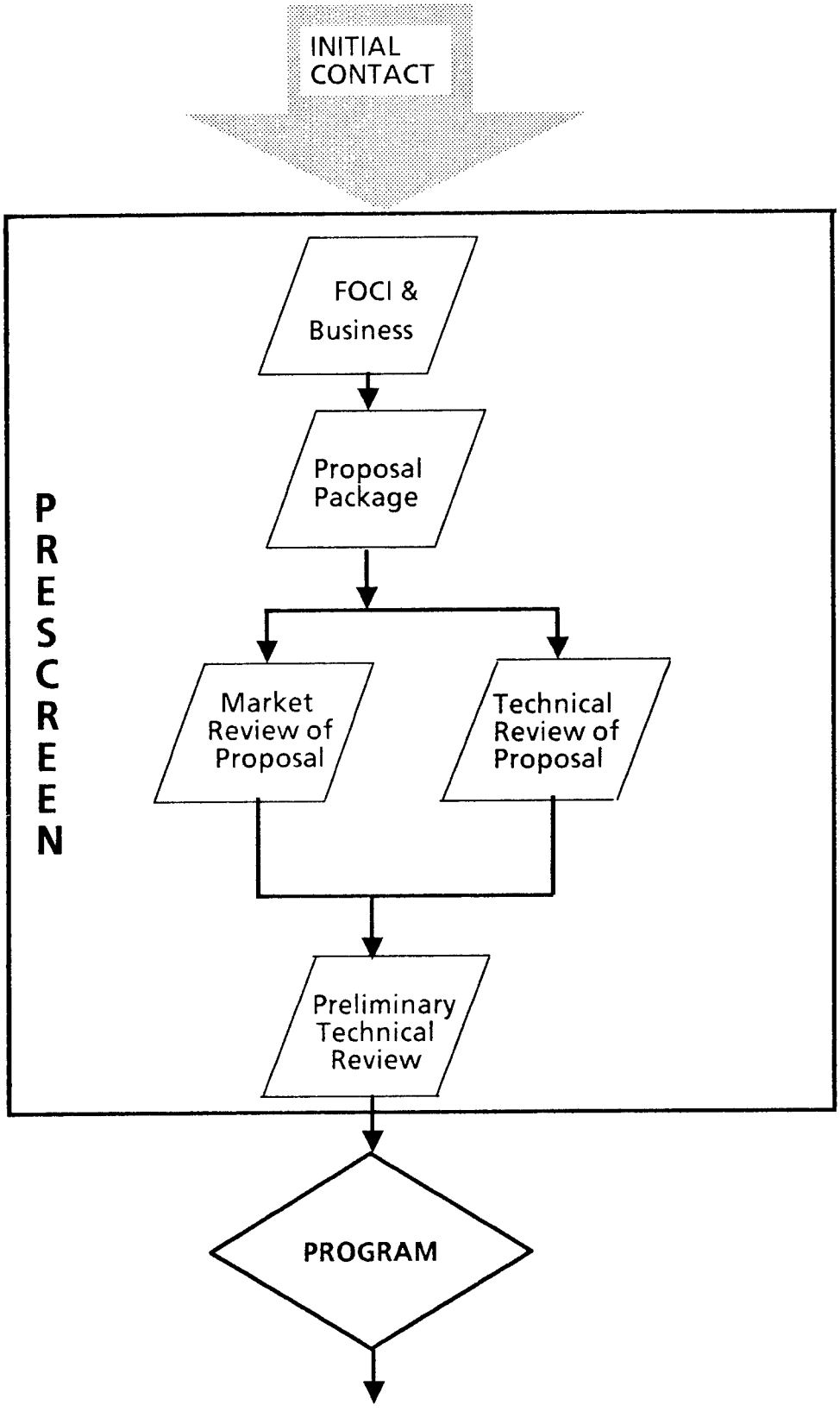


2.1 PROPOSAL REVIEW PHASE

The diagram on the following page shows the Proposal Review Phase in perspective. The following general milestones in the pre-screen process must be reached before a proposed computer product can continue in the Trusted Product Evaluation Program (additional milestones may be required):

- Initial Contact
- Certificate Pertaining to Foreign Interests (FOCI - Foreign Owned, Controlled or Influenced)
- Proposal Package Review
- Preliminary Technical Review
- Program Decision
- Legal Agreement

PROPOSAL REVIEW PHASE



2.1.1 INITIAL CONTACT

The National Security Agency's point of contact for the Trusted Product Evaluation Program is the Acquisition Policy and Business Development Branch within the Information Systems Security Organization (ISSO). We invite Interested companies to call or write to:

Director, National Security Agency
Acquisition Policy and Business Development
Attn: X511
Fort George G. Meade, Maryland 20755-6000
(301) 688-6581

2.1.2 CERTIFICATE PERTAINING TO FOREIGN INTERESTS

The National Security Agency requires that all companies submit a completed Certificate Pertaining to Foreign Interests (FOCI - Foreign Owned, Controlled or Influenced) before preparing a proposal package for the Trusted Product Evaluation Program. For those companies that may have a facility security clearance, a current DD Form 441s may be sent in lieu of the Certificate Pertaining to Foreign Interests. Please submit the certificate or DD Form 441s to the Office of Acquisition Policy and Business Development, as listed above.

2.1.3 PROPOSAL PACKAGE

The NCSC requires a separate proposal package for each computer product submitted for security evaluation. These products must be of direct and obvious benefit to the information security posture of the nation, and should address the applicable requirements outlined in the TCSEC and its interpretations. This determination will be based on the information contained in the product proposal, measured against national computer security needs and priorities.

After notification that no disqualifying foreign ownership, control or influence exists, the vendor will prepare a proposal package and provide nine copies.

The NCSC protects company proprietary information to the full extent authorized by law. The vendor must properly mark the material accordingly. The product proposal package should prove corporate-level support for the product evaluation effort and consist of a company profile, market information and a technical description of the product.

2.1.3.1 Company Profile

Potential computer security product vendors, whether requesting a system, a network, or a subsystem evaluation, must establish a formal working relationship with the NCSC. Vendors should submit as much detailed documentation as necessary to describe their company profile. Before a vendor's product is accepted in the Trusted Product Evaluation Program, the vendor must assure us that he has the potential to withstand the rigors of the evaluation process.

2.1.3.2 Market Information

To evaluate the requirements for any proposed product, the vendor must provide sufficient detail to identify its utility in the marketplace. The information below covers the minimum market information the NCSC requires to assess the probable need in the community. The market information portion of the proposal package may include the following besides other information requirements:

* Compare and contrast the proposed product and similar products that are now available showing the advantages of the proposed product.

* Intended market, including a specific customer base and firmly established requirements, by product type and level of trust.

* Portion of markets intended to address. How do you derive the specific market projections? If the product to be developed is a retrofit to existing equipment, include the potential volume of sales for those existing equipments that you already fielded.

* Known or projected U.S. Government requirements that the product will satisfy. Distinguish between DoD and civil agencies.

* Known or projected commercial requirements that the product will satisfy.

2.1.3.3 Technical Description of the Product

The NCSC needs a technical description of your product to evaluate the security features. For detailed information on product technical information consult the *Trusted Product Evaluation Questionnaire* published by the National Computer Security Center. However, the following general questions should be answered in your proposal package:

* Is your product a complete computer system or complete networking system? Does it provide some capabilities (but not all) of a computer or network system?

* Is your product primarily composed of hardware or software? Does it use both to function?

* Is your product an integral part of the entire computer or network? Did you design it to be added to a computer or network system?

* What functions does your product provide? (e.g., general purpose computer, communications switch, special purpose device)

* If your product enhances an existing computer or network system, what is the base system?

* If your product enhances an existing computer or network system, does it replace or enhance any protection features in the base system? Explain those areas that you replace or enhance.

Explain the security features provided by your product:

* What are the data containers (e.g., files, buffers, disks, process areas) in the system?

* In controlling access to data containers, are the restrictions determined on a user-by-user basis or is a system-wide policy enforced, or both?

* If you determine data container access restrictions on a user-by-user basis, to what granularity do you control or permit the sharing? (Groups of users, individual users, or both)

* Who has the authority to determine which users are capable of accessing which data containers? (System administrator, data owner, group of users associated with data, or other)

* What default protections do you provide to data containers?

* Do any data containers exist in the system that do not receive protection?

* If you base data container access restrictions on a system-wide policy, what are the rules for allowing a data container to be read and written to?

* Can these rules support the idea of a hierarchical relationship and nonhierarchical relationship? How many levels each?

* Are these rules applied to all data containers within the system?

* When the system reuses data containers, is the storage cleared before you allocate it to another user?

* When users seek to access any of the resources protected by the system, are they first required to identify and authenticate themselves?

* How do users identify themselves?

* How do users authenticate themselves?

* Is each user uniquely identified, or does the system group multiple users under a single identifier?

* Does the system audit the actions of users and administrators?

2.1.4 TYPES OF EVALUATIONS

The NCSC now conducts three distinct types of product evaluations:

1) System
2) Network
3) Subsystem

2.1.4.1 Technical Information Unique to System Evaluations

The NCSC evaluates as a system a product that addresses all the requirements of a given class of the TCSEC.

Complete information about the proposed product may not be available at this stage of the design. However, the written product proposal should answer the following questions, besides other questions, as requested:

* What is the complete technical description of the product?

* What is the targeted class or level of trust?

* What is the operating system for your product?

* What is the target development schedule? How flexible is this schedule and by what date do you plan to bring this product to market?

2.1.4.2 Technical Information Unique to Network Evaluations

The NCSC defines a network as everything needed to accomplish a job, end user to end user. The NCSC defines a network component as any part of a network. The NCSC now evaluates network products against the TCSEC as further defined in the *Trusted Network Interpretation* (TNI).

Written product proposals should answer the following questions, besides other questions, as requested:

* What is the complete technical description of the product?
* What is the underlying security policy of the product?
* What level of protection does the product provide?
* What is the projected schedule for development?
* In what environments do you intend to place the product?
* Does your product interact with users directly? If so, does it provide all the functionality identified at one of the criteria levels in Part 1 of the TNI, or only a subset?
* If it is a network system, what level of trust does it meet according to Part 1 of the TNI?
* If it is a network component, which of the following functions does it provide, and at which level of trust is each functionality provided?
    - Mandatory Access Control
    - Discretionary Access Control
    - Identification and Authentication
    - Audit
* What other security services mentioned in Part II of the TNI does your product provide?
* What type of carrier medium, if any, does your product use or support?

2.1.4.3 Technical Information Unique to Subsystem Evaluations

A computer security subsystem is a physical device or software mechanism that you add to a computer system. This subsystem enhances the computer security functionality of the total system. The NCSC now evaluates subsystem

products against the TCSEC as further defined in the *Computer Security Subsystem Interpretation* (CSSI).

To be considered for a subsystem evaluation, a company must have an existing product. This product must provide one or more of the following capabilities, as described in the CSSI:

1) Audit

2) Discretionary Access Control

3) Identification and Authentication

4) Object Reuse

Written product proposals should answer the following questions:

* What is the complete technical description of the product?

* Which of the four subsystem functions does the product implement?

* What is the current installed base? What is the projected installed base over the next five years?

* What other products does the product depend upon? (e.g., DOS, UNIX)

2.1.5 PRELIMINARY TECHNICAL REVIEW

For system and network evaluations, the NCSC will need to meet with the vendor's technical experts. This meeting will ensure that a sound technical understanding of the product forms the basis for the decision making processes. A small group of representatives from the NCSC will visit the vendor to determine the proposed product's stage of development and provide a written report. The Preliminary Technical Review (PTR) allows the NCSC to define the scope of the proposed product and to help the vendor during the Proposal Review Phase.

2.1.6 PROGRAM DECISION

The Office of Acquisition Policy and Business Development will send the company written notification when the company's proposal package is received and is under consideration. The proposal will be reviewed to determine its value. We assess 1) the capabilities of the company, 2) the utility of the product to the U.S. Government, and 3) the degree to which the product addresses the technical aspects of computer security. The availability of adequate NCSC resources to support the evaluation program is also a prime consideration in the program decision. The Office of Acquisition Policy and Business Development will notify the vendor in writing whether the product is accepted for entry into the Vendor Assistance Phase (directly into evaluation for subsystems).

2.1.7 LEGAL AGREEMENTS

When the National Security Agency accepts a package for a system or network product, they execute a legal agreement with the potential vendor whereby, inter alia:

* The National Security Agency agrees to provide necessary and relevant computer security information and guidance to the potential vendor.

* The National Security Agency agrees to protect vendor proprietary information that is provided under the legal agreement.

* The vendor agrees to provide the National Security Agency the information necessary to assess the security of the proposed product.

* The vendor agrees to follow the requirements of the procedures leading to a system, network, or subsystem evaluation.

* The National Security Agency agrees to perform an evaluation of the product with the issuance of a product rating and a final evaluation report.

* The vendor agrees to provide the U.S. Government, for approval, any company-prepared product-related brochures, advertisements, or other marketing materials which reference the National Security Agency, the TCSEC,

or the NCSC's evaluation program. These materials should be sent to the Information Security Awareness Division found under **PUBLICATIONS** as listed in the Points of Contact list at least 30 working days prior to distribution or release for publication.

* The vendor agrees to prepare a report after each Rating Maintenance Phase (RAMP) approval.

* Both parties agree to review the legal agreement periodically.

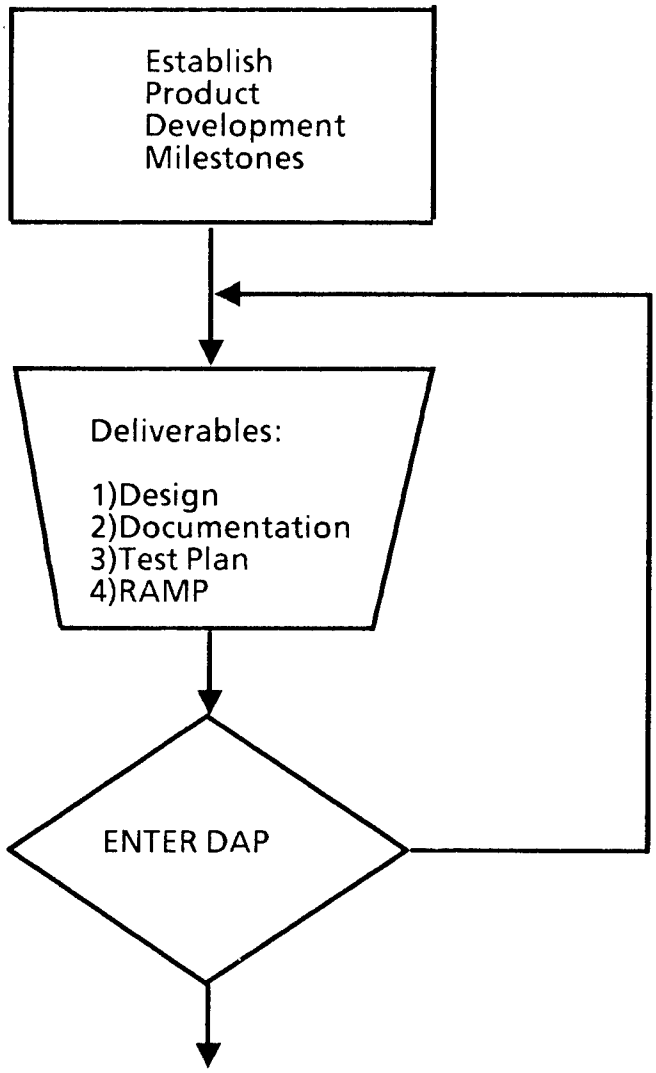
2.1.8 TEAM ASSIGNED

A program manager and a technical point of contact within the Trusted Products and Network Security Evaluations Division will be assigned to coordinate administrative and technical matters. To determine the division and class at which a computer product meets all requirements, an NCSC technical team evaluates the security of the system against the TCSEC.

2.2 VENDOR ASSISTANCE PHASE

The goal of the Vendor Assistance Phase (VAP) is to ensure that the product is ready for evaluation. The vendor will provide all necessary evidence. This phase concentrates primarily on design documentation and information supplied by the vendor, and it involves little or no "hands-on" use of the product. In addition, this phase concentrates on the development of a Rating Maintenance Plan, when applicable. Development of the product and the generation of supportive evidence can continue during this phase.

VENDOR ASSISTANCE PHASE



A firm schedule with work plans and milestones must be agreed to by both the vendor and the NCSC. The vendor must provide the following deliverables during this phase:

- Design
- Documentation
- Test Plan
- Plan for Rating Maintenance

A small team of evaluators will monitor the quality of the deliverables. To leave the Vendor Assistance Phase, three requirements must be satisfied:

a. The development cycle of the product must be within twelve months of final delivery.

b. The design must be complete.

c. Sufficient evidence must exist to support the Design Analysis Phase.

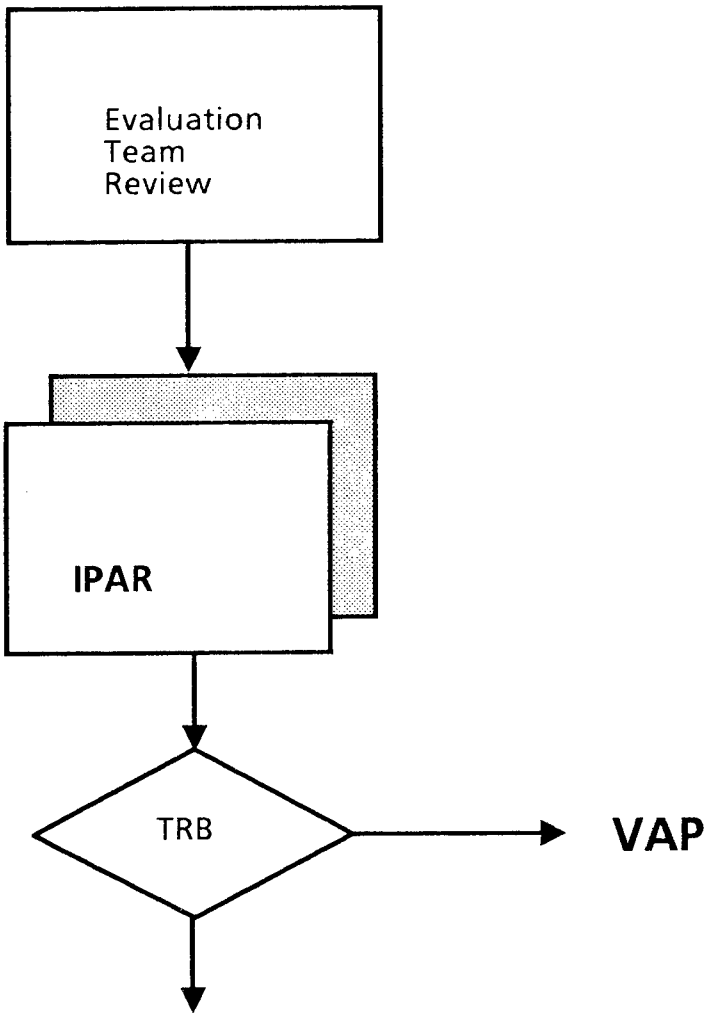
2.3 DESIGN ANALYSIS PHASE

The primary thrust of the Design Analysis Phase (DAP) is an in-depth examination of a vendor's design. This phase results in the production of an Initial Product Assessment Report (IPAR) by the evaluation team. The IPAR documents the evaluation team's understanding of the system based on the information presented by the vendor, and depicts a candidate TCSEC class rating to the system. The candidate rating is an estimate of the highest class for which the product has displayed some evidence for each of the requirements in the TCSEC.

The NCSC's Technical Review Board (TRB) examines the application of the TCSEC requirements and ensures the product is ready for evaluation. The IPAR does not represent a complete analysis of the computer product. Also, it may contain proprietary information; therefore, we restrict distribution to the particular vendor and the NCSC.

The duration of the Design Analysis Phase is not to exceed twelve months. Unsatisfactory progress during this phase will return the vendor to the Vendor Assistance Phase (VAP).

DESIGN ANALYSIS PHASE



2.4 EVALUATION PHASE

The Evaluation Phase of the Trusted Product Evaluation Program is the heart and soul of the technical evaluation process. At present, it includes three distinct types of evaluations. System and network evaluations follow the identical path, while subsystem evaluations are somewhat more abbreviated.

2.4.1 SYSTEM AND NETWORK EVALUATIONS

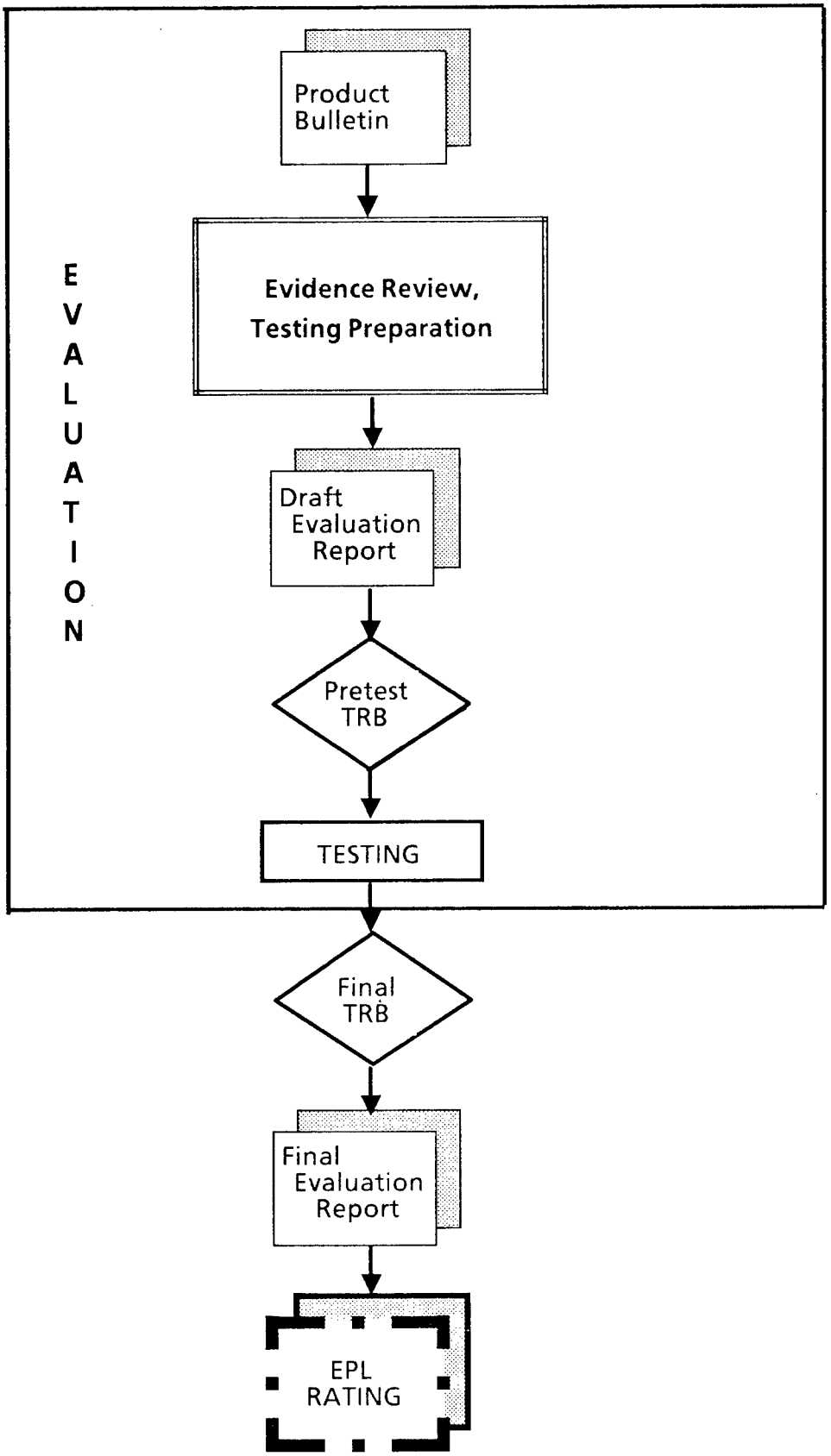
Before entering the Evaluation Phase, you must complete the design of a computer system, and it must be marketable. In addition, the product release that we evaluate must not undergo any additional development. Once the product is ready for evaluation, the NSA and the vendor sign another legal agreement. This agreement addresses the formal aspects of the product receiving an Evaluated Products List rating and the accompanying responsibilities. In addition, the responsibilities of the Rating Maintenance Phase for C1 to B1 level of trust products will also be addressed in this legal agreement.

At the start of this phase, the NCSC releases a Product Bulletin that we coordinate with the vendor. The Product Bulletin is a brief description of the computer system undergoing security evaluation and includes the candidate rating of the system. The Product Bulletin announces the evaluation in the *Information Systems Security Product and Services Catalogue*.

The Evaluation Phase is a detailed analysis of the hardware and software components of a system. It includes analysis of all system documentation and a mapping of the security features and assurances to the TCSEC. The analysis done during this phase requires "hands-on" testing (i.e., functional testing and, if applicable, penetration testing).

Before testing, the NCSC convenes a "pretest" Technical Review Board. After we complete all testing, a "final" Technical Review Board must concur on the results presented in an evaluation report.

EVALUATION PHASE



The end of the Evaluation Phase leads to the NCSC publishing a Final Evaluation Report and the Evaluated Products List entry, which are available to the public. The Final Evaluation Report summarizes the security evaluation and includes the Evaluated Products List rating. The rating is the final class at which the product successfully met all TCSEC and TNI requirements in terms of both security features and assurances. Entering the evaluation process represents a firm commitment from the vendor, and at its completion, the product will receive a rating from the NCSC.

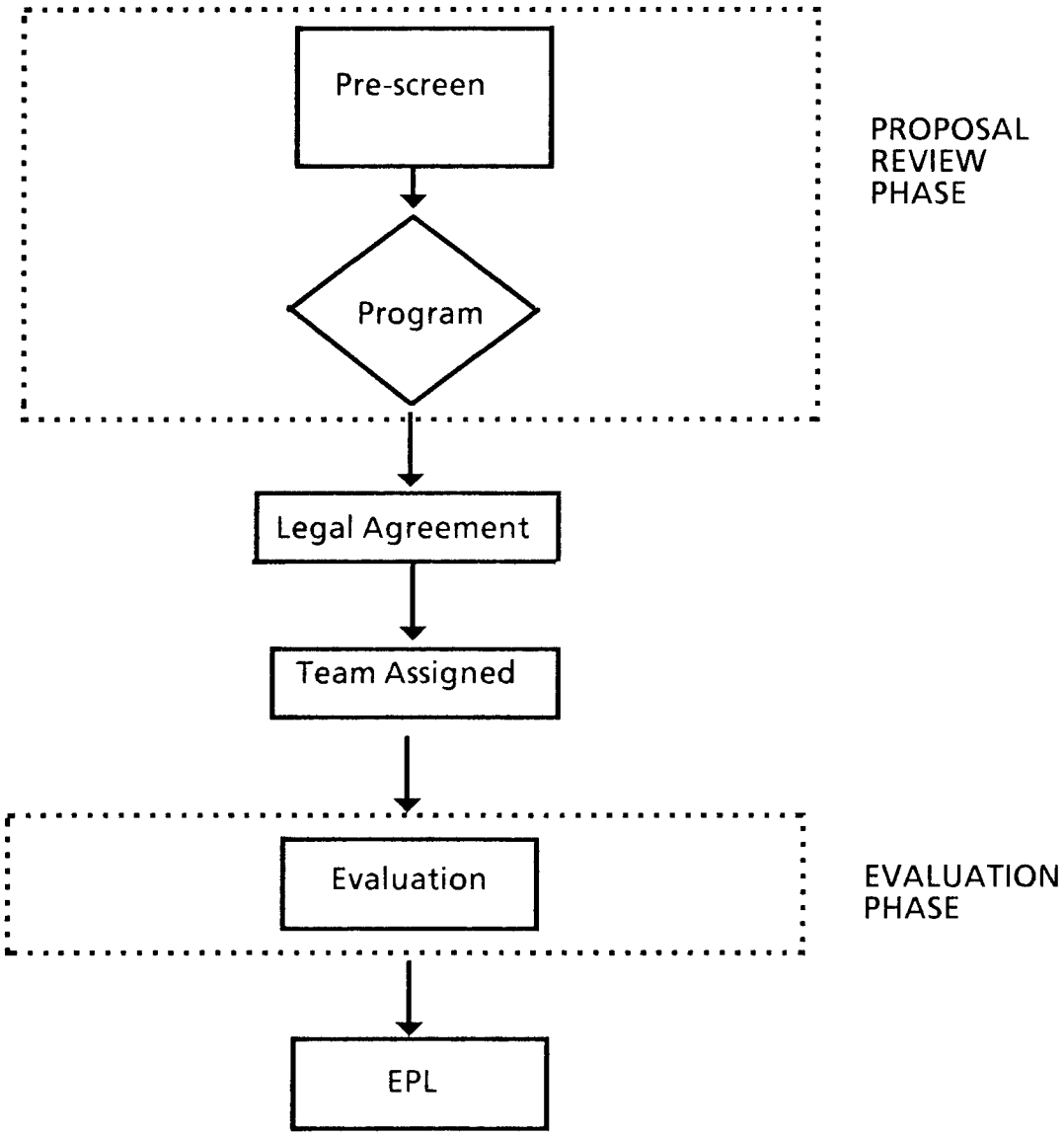
2.4.2 SUBSYSTEM EVALUATIONS

The NCSC devotes many resources to encouraging the production and use of multipurpose trusted computer systems. However, we recognize the need for guidance on, and security evaluation of, supplementary computer security products. The NCSC's subsystem evaluations provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements in existing installations. To meet this need for guidance, the NCSC has published the *Computer Security Subsystem Interpretation* and has established the subsystem evaluation process.

Once we accept a subsystem product for evaluation, the NSA and the vendor sign a legal agreement. This agreement addresses the formal aspects of the product considered for inclusion in the Evaluated Products List and the accompanying responsibilities.

Subsystems are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting automatic data processing security needs. These subsystems may not meet all the security feature, architecture, or assurance requirements of any single security class or level of the TCSEC. For the most part, we limit the scope of a subsystem evaluation to consideration of the subsystem itself. It does not address or attempt to rate the total security of the processing environment or computer system on which the subsystem may be carried. To promote consistency in evaluations, we attempt to assess a subsystem's security-relevant performance considering applicable standards and features outlined in the TCSEC. In addition, the evaluation team reviews the vendor's claims and documentation for obvious flaws

SUBSYSTEM EVALUATION



that would violate the product's security features. The team verifies, through functional testing, that the computer product does what it advertises. Upon completion, a summary of the Final Evaluation Report will be placed on the Evaluated Products List.

The Final Evaluation Report will contain a set of ratings assigned by the evaluation team to the computer subsystem based on the *Computer Security Subsystem Interpretation*. Also, the Final Evaluation Report will provide an assessment of the product's success and usefulness in increasing computer security. The Final Evaluation Report and the Evaluated Products List entry is public knowledge.

2.5 EVALUATED PRODUCTS LIST

The Evaluated Products List (EPL) provides an authoritative and unbiased security evaluation of a computer system's suitability for use in processing classified and certain unclassified information. The NCSC evaluates all products on the Evaluated Products List against the established criteria and interpretations. The rating given to a product is the highest class for which that product met or exceeded each of the individual requirements for the general evaluation class. The NCSC issues a Final Evaluation Report for all products. Reports are available from the Government Printing Office and the National Technical Information Service.

The general ratings given in the Evaluated Products List apply only to the specific hardware and software configurations listed. We scrutinized the computer product according to the detailed security testing specified in the TCSEC. However, we emphasize that such testing is not sufficient to guarantee the absence of flaws in the product. The Evaluated Products List entry does not constitute an endorsement of the product by the government. Neither does it constitute a Department of Defense certification or accreditation of the trusted computer product for use in classified or certain unclassified processing environments. Rather, the security evaluation provides an essential part of the technical evidence required for follow on certification and accreditation. Final responsibility for the continuing integrity provided by the security mechanisms of any trusted computer product evaluated by the NCSC rests solely with the vendor and the user. The Evaluated Products List, which documents evaluated computer products, is available to vendors to market and advertise actively. The general rating achieved by their products influences procurement authorities and the general public.

The Evaluated Products List contains entries for general purpose operating systems, add-on packages, and subsystems. Product Bulletins, which are synopses

of computer systems now undergoing formal security evaluations by the NCSC, are also included on the Evaluated Products List.

The *Information Systems Security Products and Services Catalogue* includes a hard copy of the Evaluated Products List. The catalogue is updated quarterly and it is available through the Government Printing Office. In addition, an electronic copy of the Evaluated Products List is available on DOCKMASTER (see Section 2.7.1).

2.6 RATING MAINTENANCE PHASE

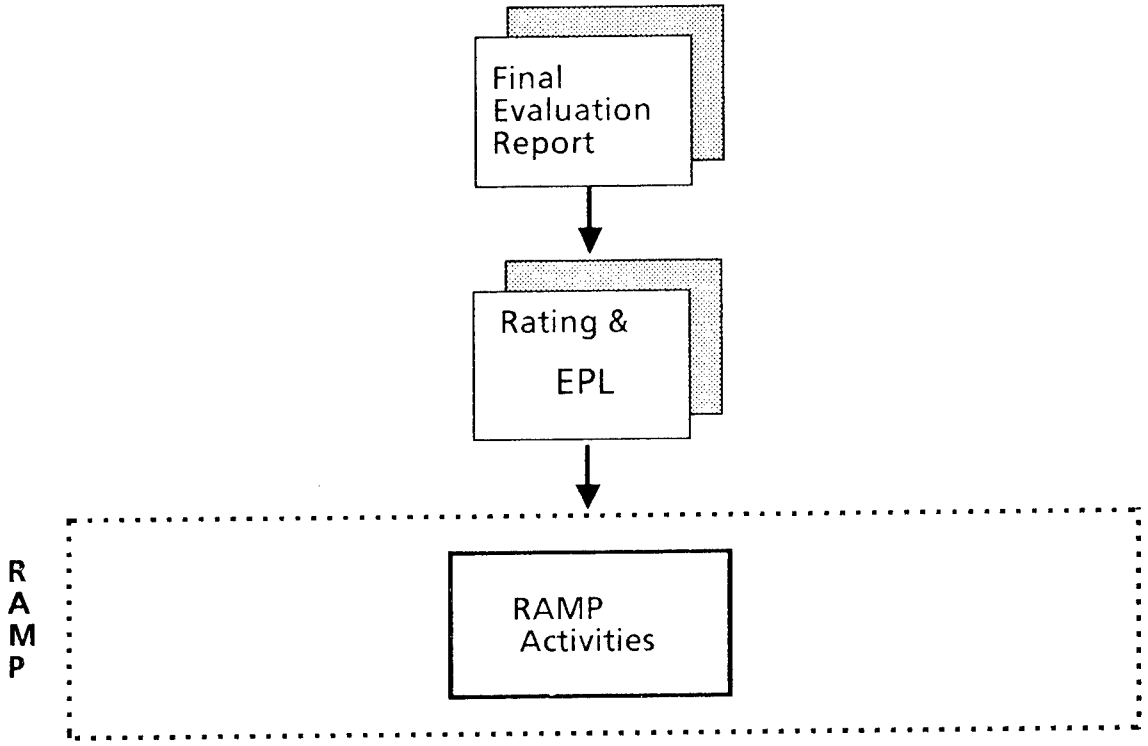
The Rating Maintenance Phase (RAMP) provides a mechanism to ensure the validity of a previous rating for a new version of an evaluated computer system product. As you make enhancements to the computer product, the Ratings Maintenance Phase ensures that the level of trust does not degrade. We require a complete reevaluation to achieve a higher rating.

The Rating Maintenance Phase keeps the Evaluated Products List current. Personnel involved in the maintenance of the product manage the change process, reducing the effort required to extend the rating. Success of the Rating Maintenance Phase depends upon the development of a cadre of vendor personnel with a strong technical knowledge of their computer product and of computer security. These trained personnel will oversee the vendor's computer product modification process. They will certify to the NCSC that any modifications or enhancements applied to the product will preserve the security mechanisms and maintain the assurances.

The Rating Maintenance Phase is initially designed for the C1 to B1 level of trust systems. As we gain experience in the program, we intend to extend this phase to higher level systems and to networks.

For additional information on this topic, the NCSC has published the *Rating Maintenance Phase - Program Document*.

RATING MAINTENANCE PHASE



2.7 EVALUATION SUPPORT SERVICES

The NCSC supports the trusted product security evaluation process within the Trusted Product Evaluation Program. The following specialized technical services are available to benefit the interactive relationship between the computer product vendors and the technical staff of the NCSC. To obtain these services or to gain more insight into their particular detail, refer to your particular interest in the Points of Contact section.

2.7.1 DOCKMASTER

DOCKMASTER is an unclassified computer system used by the NCSC for the nationwide dissemination and exchange of computer security information. DOCKMASTER serves the entire information security community including the Federal Government, universities, and private industry. It can distribute electronic mail via connections to the ARPANET. DOCKMASTER is accessible by direct dial, MILNET, and McDonnell Douglas Tymnet.

DOCKMASTER is the primary means of communications between the vendor and the NCSC throughout the computer product security evaluation process. It allows vendors to use electronic mail, file transfer protocols, and the Forum facility. Forum is an on-line, interactive meeting facility that permits an individual to "meet" with other users by using a computer terminal.

2.7.2 VERIFICATION TOOLS

Vendors who develop systems that target the class A1 requirements of the TCSEC must provide assurance that the system implementation is consistent with the system's design. You gain some of this assurance by developing a Formal Top-Level Specification of the design. You also verify that the specifications are consistent with the formal security policy model (the security requirements) for the system. After you complete the design verification, you must do an informal mapping from the Formal Top Level Specification to the implementation. This completes the evidence. Formal Top Level Specification development and later verification is a rigorous, mathematical process that can be greatly aided by automated verification tools. The TCSEC requires the use of such a tool in the verification of A1 systems. As stated, "*This verification evidence shall be consistent with that provided within the state-of-the-art of the particular 'NCSC' endorsed formal specification and verification system used.*"

We maintain the verification tools on the Endorsed Tools List that the NCSC endorses. Currently the Endorsed Tools List includes Formal Development

Methodology and Gypsy. For information about the current entries on the Endorsed Tools List, vendors should contact the ADP Applications and Services Division.

2.7.3 TECHNICAL GUIDELINES

The NCSC publishes technical guidelines that serve as additional guidance in interpreting the established standard. These technical guidelines aid in the evaluation of computer security products: complete systems, networks, and subsystems. In addition, the U.S. Government and their contractors use these technical guidelines as guidance for the procurement, use, and disposal of automated information systems and their associated magnetic storage media.

The Technical Guidelines Program contributes to the technical literature on issues of computer security. These guidelines address a demonstrated need in the automated processing environments.

Many technical experts participate in the development and review of technical guidelines: the technical staff of the NCSC and its associated offices within the National Security Agency, representatives of the Department of Defense and the Intelligence Community, civil agencies of the Federal Government, Federally Funded Research and Development Centers, contracted analytic and technical firms, and selected experts in the particular field of endeavor. We receive comments for consideration before publication.

GUIDELINES PUBLISHED BY THE NATIONAL COMPUTER SECURITY CENTER

Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC)	DoD 5200.28-STD
Department of Defense (DoD) Password Management Guideline	CSC-STD-002-85
Computer Security Requirements - - Guidance for Applying the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) in Specific Environments	CSC-STD-003-85
Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - - Guidance for Applying the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) in Specific Environments	CSC-STD-004-85
Department of Defense (DoD) Magnetic Remanence Security Guideline (FOUO) [Currently unavailable; under revision]	CSC-STD-005-85
Advisory Memorandum on Office Automation Security Guideline	NTISSAM COMPUSEC/1-87
Computer Viruses: Prevention, Detection, and Treatment	C1-Technical Report-001
A Guide to Understanding Audit in Trusted Systems	NCSC-TG-001
Trusted Product Evaluations: A Guide for Vendors	NCSC-TG-002
A Guide to Understanding Discretionary Access Control (DAC) in Trusted Systems	NCSC-TG-003

Glossary of Computer Security Terms	NCSC-TG-004
Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC)	NCSC-TG-005
A Guide to Understanding Configuration Management in Trusted Systems	NCSC-TG-006
A Guide to Understanding Design Documentation in Trusted Systems	NCSC-TG-007
A Guide to Understanding Trusted Distribution in Trusted Systems	NCSC-TG-008
Computer Security Subsystem Interpretation (CSSI) of the Trusted Computer System Evaluation Criteria (TCSEC)	NCSC-TG-009
Trusted Network Interpretation Environments Guideline	NCSC-TG-011
Rating Maintenance Phase (RAMP) - Program Document	NCSC-TG-013
Guidelines for Formal Verification Systems	NCSC-TG-014
A Guide to Understanding Trusted Facility Management	NCSC-TG-015
Trusted Product Evaluation Questionnaire	NCSC-TG-019
Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System	NCSC-TG-020-A
Information Systems Security Products and Services Catalogue	Quarterly Updates

The Standards, Criteria, and Guidelines Division is continuously adding new technical guidelines to the Rainbow Series.

2.7.4 COMPUTER SECURITY TECHNICAL PUBLICATIONS

The NCSC publishes various technical publications that are useful to a vendor for general computer security awareness, as well as to process a computer product through the Trusted Product Evaluation Program. The Information Security Awareness Division will provide copies in limited quantity upon request.

2.7.5 TRAINING

The NSA provides training on topics of major importance to vendors interested in the trusted product security evaluation process.

2.7.6 OTHER RELATED SERVICES

Within the Information Systems Security Organization, several separate, but complementary, programs relate to the Trusted Product Evaluation Program. The following paragraphs provide a brief description of each program. For more details, please contact the specific program office in the Points of Contact list.

Like the Trusted Product Evaluation Program, the Commercial Communications Security Endorsement Program is a partnership with private industry. It combines private sector leadership and expertise in equipment design, development and high volume production with the information security expertise of the National Security Agency. Specifically, the National Security Agency designed this program to encourage industry to embed U.S. Government cryptography into telecommunications products to protect classified and certain unclassified information. In today's computer networking environment, many products require both an encryption capability and a trusted computing base to meet user requirements. Companies whose products merge both communications and computer security disciplines should benefit from becoming familiar with the requirements of the Commercial Communications Security Endorsement Program.

The National Security Agency established the Secure Data Network System Program in August 1986. We joined in partnership with ten major telecommunications and computer companies to develop a security architecture and

a user-friendly key management system using the Open Systems Interconnection model. The Secure Data Network System Program provides for the development of information security products that can operate over a broad range of commercial data networks.

To aid industry in developing and testing TEMPEST-suppressed equipment that can be offered for sale to the U.S. Government, the National Security Agency administers the TEMPEST Endorsement Program. Companies developing trusted computing products should be aware that the U.S. Government may require that products protecting classified information be TEMPEST-suppressed.

Vendors who are developing trusted computer products as Independent Research and Development Projects may obtain technical assistance. You can reach the Technical Staff of the Information Systems Security Research and Technology Group for information on technical plan evaluations.

The Department of Defense (DoD) established the Computer Security Technical Vulnerability Reporting Program (CSTVRP) to maintain a central repository of vulnerability information. The Information Systems Security Organization in the National Security Agency is responsible for instituting the CSTVRP as directed by DoD Instruction 5215.2 on 2 September 1986. The Instruction applies DoD-wide, including the Office of the Secretary of Defense, the Military Departments, the Joint Chiefs of Staff, all Commands, and all Defense Agencies. The CSTVRP provides a mechanism for reporting weaknesses or design deficiencies in hardware, firmware, or software that leave automated information systems open to potential exploitation. Technical vulnerabilities reported in evaluated computer products, listed on the Evaluated Products List, could possibly change the general rating of the product.

POINTS OF CONTACT

COMMERCIAL COMMUNICATIONS SECURITY ENDORSEMENT PROGRAM

Director, National Security Agency
Acquisition Policy and Business Development
Attention: X511
Fort George G. Meade, MD 20755-6000
(301) 688-6581

COMPUTER SECURITY TECHNICAL VULNERABILITY REPORTING PROGRAM

Director, National Security Agency
Computer Security Technical Vulnerability Reporting Program
Attention: DDI/CSTVRP
Fort George G. Meade, MD 20755-6000
(301) 688-6079

DOCKMASTER AND VERIFICATION TOOLS

Director, National Security Agency
ADP Applications and Services
Attention: C83
Fort George G. Meade, MD 20755-6000
(301) 859-4360

INDEPENDENT RESEARCH AND DEVELOPMENT PROJECTS

Director, National Security Agency
Information Systems Security Research and Technology
Attention: R206
Fort George G. Meade, MD 20755-6000
(301) 859-6515

PUBLICATIONS

Superintendent of Documents
U.S. Government Printing Office
Washington, DC 20402
(202) 783-3238

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650

Director, National Security Agency
Information Security Awareness
Attention: X713
Fort George G. Meade, MD 20755-6000
(301) 688-8742, or
(301) 766-8729

SECURE DATA NETWORK SYSTEM PROGRAM

Director, National Security Agency
Multilevel Security Workstations
Attention: V531
Fort George G. Meade, MD 20755-6000
(301) 859-4387

TECHNICAL GUIDELINES PROGRAM

Director, National Security Agency
Standards, Criteria, and Guidelines
Attention: C81
Fort George G. Meade, MD 20755-6000
(301) 859-4463

TEMPEST ENDORSEMENT PROGRAM

Director, National Security Agency
TEMPEST Endorsement Program
Attention: X512
Fort George G. Meade, MD 20755-6000
(301) 688-8728

TRUSTED PRODUCT EVALUATION PROGRAM

Director, National Security Agency
Acquisition Policy and Business Development
Attention: X511
Fort George G. Meade, MD 20755-6000
(301) 688-6581

BIBLIOGRAPHY

Computer Security Evaluation Center, DoD Directive 5215.1, 25 October 1982.

Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-009 Version 1, 16 September 1988.

Computer Security Technical Vulnerability Reporting Program, DoD Instruction 5215.2, 2 September 1986.

Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985; supersedes CSC-STD-001, dated 15 August 1983.

Independent Research and Development, Under Secretary of Defense for Research and Engineering, DoD 3204.1, 1 December 1983.

National Policy on Controlled Access Protection Policy, National Telecommunications and Information System Security Policy No. 200, 15 July 1987.

Rating Maintenance Phase - Program Document, NCSC-TG-013 Version 1, 23 June 1989.

Security Requirements for Automatic Data Processing (ADP) Systems, DoD Directive 5200.28, revised April 1978.

Trusted Network Interpretation of The Trusted Computer System Evaluation Criteria, NCSC-TG-005 Version 1, 31 July 1987.

Trusted Product Evaluation Questionnaire, NCSC-TG-019 Version 1, 16 October 1989.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	22 June 1990	Final ; supersedes draft version, 1 March 1988

4. TITLE AND SUBTITLE
TRUSTED PRODUCT EVALUATIONS: A GUIDE FOR VENDORS

5. FUNDING NUMBERS

6. AUTHOR(S)
NCSC and ISSO Ad Hoc Working Group

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Security Agency
Standards, Criteria, and Guidelines ATTN: C81
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

8. PERFORMING ORGANIZATION REPORT NUMBER
NCSC-TG-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Security Agency
Blaine W. Burnham Chief C81
Fort George G. Meade, MD 20755-6000
(301) 859-4463

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
LIBRARY No.: S-228,538

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release:
Distribution Unlimited

12b DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The *Trusted Product Evaluations: A Guide for Vendors* addresses the procedures for the vendor interacting with the National Security Agency's Information Systems Security Organization as the vendor relates to the Trusted Product Evaluation Program within the National Computer Security Center (NCSC). It provides, in essence, what the vendor needs to know in order to submit a product for technical evaluation and it outlines the Agency's responsibilities for positive, timely acknowledgments. It specifically covers the Agency's relationship with vendors of proposed trusted computer products from the initial contact through the rating process in the Final Evaluation Report. Although more detailed instructions are referenced in this publication, sufficient guidelines are established for any first time user of the NCSC's services.

14. SUBJECT TERMS	15. NUMBER OF PAGES
National Computer Security Center, Trusted Computer System Evaluation Criteria (TCSEC), Computer Security Evaluation, Trusted Product Evaluation Program, Technical Guideline.	**37**
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	**UNCLASSIFIED**	**UNCLASSIFIED**	